IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF** **J. ALEX HALDERMAN IN** **SUPPORT OF MOTION FOR** **PRELIMINARY INJUNCTION** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

Georgia’s Current Election Technology

2. Georgia recently deployed new voting equipment and software manufactured by Dominion Voting Systems, Inc. (“Dominion”). These components include ImageCast X Prime (“ICX”) ballot marking devices (“BMDs”), ImageCast Precinct (“ICP”) precinct-count scanners, ImageCast Central (“ICC”) central-count scanners, and the Democracy Suite election management system (“EMS”). Georgia

Secretary of State Brad Raffensperger certified these components in August 2019,[1] and they were first used statewide during the June 20, 2020 election.[2]

3. Under this new system (the "BMD-based Election System"), Georgia generally requires all in-person voters to select candidates on Dominion ICX BMDs. These devices are computer tablets connected to off-the-shelf laser printers. They do not record votes but instead print paper records that are supposed to contain the voter's selections in both human-readable text and as a type of machine-readable barcode called a QR code. Voters insert these printouts into Dominion ICP optical scanners, which read the barcodes and count the votes encoded in them.[3]

4. Absentee voters do not use BMDs but instead complete hand-marked paper ballots ("HMPBs"), which are tabulated at central locations by Dominion ICC scanners. While Georgia's precinct-based ICP scanners have the capability to count hand-marked paper ballots,[4] the State only uses them to count BMD printouts.

[1] Georgia Dominion certification (Aug. 9, 2019), https://sos.ga.gov/admin/uploads/Dominion_Certification.pdf.

[2] Mark Niesse, "How Georgia's new voting machines work," *The Atlanta Journal-Constitution* (June 9, 2020), https://www.ajc.com/news/state--regional-govt--politics/how-georgia-new-electronic-voting-machines-work/RyIOJuHYQgktcCNGL9sEoK/.

[3] Decl. of Dr. Eric Coomer, Dckt. 658-2, at 10.

[4] *Id* at 9.

5. Pre- and post-election procedures in the BMD-based election system closely parallel those under the old DRE-based election system. Before every election, the Secretary of State's office prepares election programming files using Dominion EMS software, which is a collection of client and server programs that run on commercial-off-the-shelf (COTS) computers and servers. The Secretary of State transmits the election programming files to county officials, who use another instance of the Dominion EMS to prepare memory cards and USB sticks for every scanner and ballot marking device used in the county. These removable media contain the ballot design, including the names of the races and candidates, and rules for counting the ballots. Election workers install a memory card or USB stick into each BMD and ICP scanner prior to the start of voting.

6. After polls close, election workers remove the memory cards from every ICP scanner and return them to the county. At that point, the memory cards contain a digital image of each scan as well as the scanner's interpretation of the votes contained in the barcode. County workers use the Dominion EMS to retrieve data from the cards and prepare the final election results based on the barcode readings.

Attacks Against the BMD-based Election System

7. Attackers could alter election outcomes under Georgia's BMD-based election system in several ways:

(a) Attacks on the BMDs could cause them to print barcodes that differ from voters' selections. These changes would be undetectable to voters, who cannot read the encrypted barcodes. Since the barcodes are the only thing the scanners count, the impact would be a change to the election results. The only known safeguard that can reliably detect such an attack is to rigorously audit both the human-readable portion of the printouts and the barcodes, which Georgia does not currently do.

(b) Attacks on the BMDs could also change *both* the barcode and the human-readable text on some of the printouts. Research shows that few voters carefully review their BMD printouts, and, consequently, changes to enough printouts to change the winner of a close race would likely go undetected. No audit or recount could detect this fraud, since both the digital and paper records of the votes would reflect the same selections but not the ones the voters intended.

(c) Attacks on the scanners could also cause fraudulent election results by changing the digital records of the votes. The only known safeguard that can reliably detect such an attack is a sufficiently rigorous manual audit or recount of the paper records, which Georgia does not currently require.

8. One way that attackers could carry out attacks against the BMD-based election system is by infecting the election equipment with malicious software ("malware"). Malware could potentially be introduced in several ways, including: (a) with physical access to any of the many electronic components that compose the system, (b) through an attack on the hardware or software supply-chain, or (c) by spreading virally via the election management systems to polling place equipment during routine pre-election procedures.

9. Components of Georgia's election system that are not directly connected to the Internet might nonetheless be targeted by attackers. Nation-state attackers have developed a variety of techniques for infiltrating non-Internet-connected systems, including by spreading malware on removable media that workers use to copy files in and out.[5] Attackers could employ this method to infect the state or county EMS and spread from there to scanners and BMDs when workers program them for the next election. In this way, an attack could potentially spread from a single point of infection to scanners and BMDs across entire counties or the whole

[5] A well-known example of this ability, which is known as "jumping an air gap," is the Stuxnet computer virus, which was created to sabotage Iran's nuclear centrifuge program by attacking factory equipment that was not directly connected to the Internet. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired* (Nov. 3, 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

state, in the same way that malware could have spread through the old DRE system, which was not effectively air-gapped or otherwise reasonably secured.

10. The BMD-based election system is at further heightened risk of attack because of the legacy of poor security in Georgia's old DRE-based election system and its associated computers and networks. If attackers infiltrated the DRE-based system, they likely did so by first infiltrating components such as the Secretary of State's computer network, the voter registration database software developed by PCC, Inc., or the non-"air gapped" computers and removable media used by state and county workers and outside contractors to transfer data into and out of the EMS. The record in this matter contains abundant evidence about vulnerabilities in all these components, some of which were unmitigated for years and may still be unmitigated. Responsibility for their security continues to rest with many of the same technicians and managers who oversaw the security of the old system and were unable or unwilling to implement effective security measures.

11. These components continue to be used with the new voting system, including to process data that is copied to polling-place equipment. If attackers breached any of them to attack the DRE-based system, those attackers may continue to have such access under the BMD-based system. Technologies that the State has highlighted as key defenses for these legacy components, such as anti-malware

scans, anti-virus scans, and endpoint protection, provide little defense against sophisticated attackers like hostile foreign governments.

12. Importantly, apart from the examinations Fortalice conducted that found significant vulnerabilities with the Secretary of State's information technology infrastructure including components of the election management network, there is no indication that Georgia has ever forensically or otherwise rigorously examined the current election system, including components from the prior DRE-based system that are used with the current BMD-based system. In an environment of advanced persistent threats to both election systems, coupled with the critical known vulnerabilities with those systems, the lack of any such examination raises serious concerns about the reliability of the current system and election outcomes.

Georgia's New Dominion Equipment has Critical Security Flaws

13. Dominion does not dispute that its products can be hacked by sufficiently capable adversaries.[6]

14. One reason why this is true is the complexity of the software, which far exceeds the complexity of the DRE-based system. The Dominion software used in

[6] Decl. of Dr. Eric Coomer, Director of Product Strategy and Security for Dominion ¶ 13, Dckt. No. 658-2 ("all computers can be hacked with enough time and access").

Georgia contains nearly 2.75 million lines of source code (equivalent to about 45,000 printed pages), excluding the Windows and Android operating systems and other off-the-shelf software packages.[7] The ICP scanner alone contains about 475,000 lines of source code, and its software is written in C/C++,[8] a programming language that is particularly susceptible to some of the most dangerous types of vulnerabilities.

15. Software of the size and complexity of the Dominion code inevitably has exploitable vulnerabilities. As a source-code review team working for the California Secretary of State concluded in a study of a voting system with only 10% as much code as Dominion's, "If the [system] were secure, it would be the first computing system of this complexity that is fully secure."[9] Nation-state attackers often discover and exploit novel vulnerabilities in complex software.[10]

[7] SLI Compliance, "Dominion Democracy Suite 5.10 Voting System Software Test Report for California Secretary of State" (Aug. 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510software-report.pdf.

[8] *Id.*

[9] Joseph A. Calandrino, Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, and William Zeller, "Source Code Review of the Diebold Voting System," in *California Secretary of State's Top-to-Bottom Review of Voting Systems* (July 20, 2007), https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-source-public-jul29.pdf.

[10] Andrew Springall, *Nation-State Attackers and their Effects on Computer Security* (2019), Ph.D. dissertation, University of Michigan, https://deepblue.lib.umich.edu/handle/2027.42/143907.

16. In addition to its complexity, the Dominion software used in Georgia utilizes a wide range of outdated off-the-shelf software modules, including some that perform essential security functions, such as the operating system and modules that process files an attacker might have manipulated.[11] The oldest third-party software components appear not to have been updated in more than 15 years. This is unfortunately consistent with the DRE-based system, which relied on software so out of date that the manufacturer stopped providing updates and patches more than a decade ago.

17. Outdated software components are a security risk because they frequently contain known, publicly documented vulnerabilities that have been corrected in later versions. Old or outdated software used in Georgia's Dominion equipment includes a version of Microsoft SQL Server dating from 2016, Adobe Acrobat from around 2015, barcode scanner software from 2015, µClinux operating system software from 2007, COLILO bootloader software from 2004, and a version of the Apache Avalon component framework dating from 2002. Georgia's BMDs

[11] SLI Compliance, "Dominion Voting Systems Democracy Suite 5.5-A Certification Test Plan" 16-19 (Dec. 2018), https://www.eac.gov/sites/default/files/voting_system/files/DVS_Democracy_D-Suite_5.5-A_Modification_Test_Plan_v1.2.pdf.

use the Android 5.1.1 operating system,[12] which is almost six years old and has not received security updates since March 2018; as of August 2020, it contained 254 documented vulnerabilities.[13]

18. Georgia certified the Dominion system without performing its own security testing or source-code review. The certification was preceded by tests that were limited to checking functional compliance with Georgia requirements.[14] The test report states that the testing "was not intended to result in exhaustive tests of system hardware and software attributes."[15] The term "security" does not appear in the report.

19. Several months before Georgia certified the Dominion system, the State of Texas performed its own certification tests. The Texas certification was more comprehensive and included test reports from five examiners appointed by the Texas

[12] Certificate of Conformance, Dominion Voting Systems Democracy Suite 5.5-A (Jan. 30, 2019) at pp. 3-4, https://www.eac.gov/file.aspx?A=TQycVTA%2BOLpxoCbwCFjQJmJdRP1dq9sFO3oVUWJl5u4%3D.

[13] CVE Details, "Google Android 5.1.1 Security Vulnerabilities," https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/version_id-186573/Google-Android-5.1.1.html (last visited Aug. 19, 2020).

[14] Pro V&V, "Test Report: Dominion Voting Systems D-Suite 5.5-A Voting System Georgia State Certification Testing" (Aug. 7, 2019), https://sos.ga.gov/admin/uploads/Dominion_Test_Cert_Report.pdf.

[15] *Id*. at 3.

Secretary of State.[16] All of the examiners highlighted deficiencies with the Dominion system, including issues affecting its reliability, accessibility, and security. These problems led Texas to deny certification of the Dominion system in 2019.[17]

20. Several of the serious deficiencies noted by the Texas examiners affect system components used in Georgia, including the BMDs. One examiner noted that "the ICXs [BMDs] are built with a [commercial off-the-shelf] tablet and printer. The Android OS versions used on the tablets are several years old[;] therefore they do not have the latest security feature [*sic*.] as later Android releases."[18] A second examiner found that "[t]he doors covering data and power ports on the [BMD] tablets do not provide sufficient protection. […] a bad actor could add a USB device to the tablet while powered down that could remain undetected until after the election had ended."[19] A third examiner concluded that "[t]he ICX [BMD] also presented problems during the accessibility testing portion of the exam which demonstrate that it may not be suitable as an accessible voting system."[20]

[16] "Examiner Reports of Dominion Voting System Democracy Suite 5.5" (Jan. 16-17, 2019), https://www.sos.state.tx.us/elections/laws/jan2019_dominion.shtml.

[17] "Report of Review of Dominion Voting Systems Democracy Suite 5.5" (June 20, 2019), https://www.sos.state.tx.us/elections/forms/sysexam/dominion-democracy-suite-5.5.pdf

[18] Report of Texas examiner Tom Watson.

[19] Report of Texas examiner Brian Mechler.

[20] Report of Texas examiner Chuck Pinney.

21. Around the same time that Georgia certified the Dominion system, the State of California performed tests on a more recent version of the Dominion software, version 5.10, as part of its own certification process.[21]

22. In contrast to Georgia's tests, California's included some source code review and security testing. Like all security testing, the California tests were necessarily limited in scope and could not be expected to find all exploitable vulnerabilities. Nevertheless, they did uncover several serious flaws. These problems very likely apply to the version of the Dominion system used in Georgia given that it precedes the version tested in California.

23. The California testers found that attackers could modify the Dominion software installation files and believed that "it would be possible to inject more lethal payloads into the installers given the opportunity."[22] This implies that attackers could modify the Dominion installation files to infect election system components with malicious software.

[21] SLI Compliance, "Dominion Democracy Suite 5.10 Security and Telecommunications Test Report" (Aug. 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510security-report.pdf ("California Certification Security and Telecomm Test Report").
[22] *Id*. at 25.

24. Furthermore, the California testers found that the Dominion system's antivirus protection was insufficient or non-existent. "[O]n the EMS server, the AVAST Antivirus (AV) File Shield (the real time AV monitor) was only able to detect and clean one of the four [test] files. This potentially leaves the system open to zipped and double zipped viruses as well as infection strings in plain text."[23] Moreover, the ICX BMD and ICP scanner have no antivirus software at all.[24] As a result, malware that infected the Dominion components could evade antivirus detection.

25. One of the ways that attackers might affect election equipment is by physically accessing the devices. In the case of the Dominion BMD, the California source code reviewers found a vulnerability that can be exploited with physical access to the USB port that "would be open to a variety of actors including a voter, a poll worker, an election official insider, and a vendor insider."[25] This implies that no passwords or keys would be needed to exploit the problem, given physical access. California testers also found that "the ICX device does not provide monitoring of

[23] *Id*. at 19-20.
[24] *Id*. at 20.
[25] California Secretary of State's Office of Voting Systems Technology Assessment, "Dominion Voting Systems Democracy Suite 5.10 Staff Report" (Aug. 19, 2019) at 29, https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510staff-report.pdf.

physical security,"[26] and that, for all the polling place devices, including the ICX, "[s]ecurity seals, locks, and security screws can be circumvented."[27]

26. Other weaknesses found in the California tests include that "a number of passwords were able to be recovered that were stored in plain text,"[28] that the network switch used to connect EMS clients and servers was "determined to have twelve medium [severity] vulnerabilities and four low [severity] vulnerabilities,"[29] and that, if an authentication device used by poll workers and administrators was lost or stolen shortly before an election, revoking its access would require a logistically difficult process to reprogram the election files for the polling place devices throughout the jurisdiction.[30] These problems indicate that the Dominion system was designed without sufficient attention to security.

27. Although California ultimately permitted the Dominion system to be used, its certification requirements impose much more stringent security conditions

[26] California Certification Security and Telecomm Test Report at 11.

[27] *Id*. at 17.

[28] *Id*. at 15.

[29] *Id*. at 30.

[30] *Id*. at 15.

than those in Georgia, and no California jurisdiction uses Dominion BMDs for all voters as Georgia does.[31]

28. Dominion's response to Georgia's RFP lists among "key personnel" a "Chief Security Officer" (CSO) whose responsibilities for the voting system project were to be "Oversight of key security development and implementation."[32] Appointing a C-level executive to oversee a company's security posture is widely regarded as an industry best practice. However, at the time of the RFP, the CSO position was vacant, and to my knowledge Dominion has yet to fill the role.

<u>BMDs and Ballot Barcodes Create Elevated Hacking Risks</u>

29. Georgia's optical scanners use barcodes as the exclusive means of reading voters' choices. This increases the likelihood that attackers will be able to manipulate election results. The use of barcodes makes it possible for attackers to change how votes are recorded by hacking *either* the scanners or the BMDs. This

[31] California Secretary of State, "Conditional Approval of Dominion Voting Systems, Inc. Democracy Suite Version 5.10 Voting System" (Oct. 18, 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds510-cert.pdf.

[32] See "Original\0-4 Org Structure_Dominion and KNOWiNK - Redacted .pdf" at 3 *available at* https://sos.ga.gov/admin/uploads/Dominion.zip (last visited Aug. 19, 2020).

increases the “attack surface” of the election system: with two potentially vulnerable components to target instead of just one, attackers are more likely to succeed.

30. Georgia’s Dominion ICX BMDs are computers, they run outdated and vulnerable software, and they must be programmed using the State’s election management system before every election. Attackers could potentially infect Georgia’s BMDs with malware in several ways, including by spreading it from the election management system (EMS).

31. An attacker who infected the BMDs with malware could change a fraction of the printouts so that the barcodes encoded fraudulent votes but the human-readable text showed the voters’ true selections.

32. Voters would have no way to detect this attack. They cannot read the Dominion barcodes, which are encrypted, so it is impossible for them to verify whether the barcodes really match their selections. However, when the Dominion scanners tabulate BMD printouts, they ignore the printed text entirely and count only the votes encoded in the barcodes. This means that voters cannot verify the portion of their ballots that gets counted.

33. Such barcode attacks cannot be reliably detected using pre-election testing or parallel testing.[33] An attacker could decide which votes to modify based on a very large number of variables, including the time of day, the number of ballots cast, the voter's selections, and whether the voter used options such as a large font size or an audio ballot. It is impossible for any practical amount of testing to examine all sets of conditions under which attackers might choose to cheat.

34. In principle, a sufficiently rigorous audit that compared the human-readable portion of the printouts to the barcodes could detect such an attack. However, since attackers might choose to target any race in any election, every race and every election would need to be rigorously audited to rule out barcode-based fraud.

35. To my knowledge, Georgia has not announced plans to perform any kind of audit that would compare the barcodes and the printed text, nor what specific measures would be taken to render any potential audit sufficiently comprehensive and reliable.

36. Even if officials did detect that some ballots showed different choices in the barcode than in the text, there might be no way to determine the correct election

[33] *See* Philip B. Stark and Ran Xie, "Testing Cannot Tell Whether Ballot-Marking Devices Alter Election Outcomes" (2020), https://arxiv.org/pdf/1908.08144.pdf.

results. If the discrepancies resulted from an attack, this would cast doubt on *both* the barcodes and the ballot text. An attacker who was able to alter the barcode would be equally capable of altering the ballot text. Malware might be designed to sometimes alter only the barcode and sometimes only the text. This means that officials could not simply ignore the barcodes and count only the text if they suspected the BMDs had been compromised.

37. BMDs do not need to use barcodes. Several kinds of modern, EAC-certified BMDs deployed in other states do not use barcodes to encode votes. These include the Clear Ballot ClearAccess system[34] and the Hart Verity Touch Writer.[35] Instead of a barcode for vote tabulation, these systems print a ballot that looks like a hand-marked paper ballot but has scan targets filled in for the selected candidates.

38. In Dominion's response to the State's request for proposals, the company represented that an upcoming version of its BMD software would not need to print barcodes on ballots.[36] Instead, the BMDs would produce (and the scanners

[34] *See* Clear Ballot, "ClearAccess Accessible Voting," https://clearballot.com/products/clear-access.

[35] *See* Hart Intercivic, "Verity Touch Writer Ballot Marking Device," https://www.hartintercivic.com/wp-content/uploads/VerityTouchWriter.pdf.

[36] "Clarification Questions\MS 16-1 Supply Chain_Dominion and KNOWiNK Final.docx" *available at* https://sos.ga.gov/admin/uploads/Dominion.zip (last visited Aug. 19, 2020).

would count) an entirely human-readable ballot capable of verification by the voter. However, this option is described as an "upgrade" available only after "certification is complete at the EAC."

39. The Secretary of State's office and Dominion portray Georgia's BMDs as having this ability to print such a human-readable, "full-face" ballot. A video portraying such a capability is part of the "Important Voter Information" available to the public on the Secretary of State's elections security web page.[37] The video portrays a voter making her selections on a BMD displaying a mock ballot using Georgia state and local races and constitutional questions or referenda. At the end of the video, the voter selects "Print Ballot," and the attached printer produces a double-sided ballot with a darkened oval appearing next to the voter's selections.[38]

40. Dominion's in-precinct optical scanners already are capable of and certified to read such full-face paper ballots that do not encode votes using barcodes.

[37] https://www.dropbox.com/s/u0lc21u82ye2qpg/ICX%20BMD%20Cart.mp4, available through "Voting Cart" hyperlink at https://sos.ga.gov/securevoting (last visited Aug. 18, 2020).

[38] *Id.*

BMDs Limit the Effectiveness of Voter Verification

41. Even if Georgia were to implement rigorous post-election audits, BMDs make it possible for an attacker to compromise the auditability of the ballots and thereby undermine the primary goal of the paper trail. To do so, malware would cause the BMDs to sometimes print fraudulent selections in *both* the barcode and the human-readable text. This attack would be impossible to detect by auditing the printouts, because all records of the voter's intent would be wrong. Pre-election testing and parallel testing also cannot reliably detect such cheating.

42. Unlike the security of hand-marked paper ballots, the security of BMDs relies critically on voters themselves. The only practical way to discover a BMD attack that altered both the barcodes and the printed text would be if enough voters reviewed the printouts, noticed the errors, and alerted election officials. Yet several recent studies, including my own peer-reviewed research, have concluded that few

voters carefully review BMD printouts.[39,40,41] As a result, the BMD paper trail is not a reliable record of the votes expressed by the voters, and changes to enough printouts to change the winner of a close race would likely go undetected.

43. Even if some voters did notice that their selections were misprinted, these voters would have no way to prove that the BMDs were at fault. From an election official's perspective, the reporting voters might be mistaken or lying. Many voters would need to report that the BMDs misprinted their ballots before officials could be sure there was a systemic problem.

44. There are no protocols or policies in Georgia that I have found that address how many voter complaints, or other conditions, involving BMDs would be required within or across polling places to support a finding—or even a robust investigation—of a systemic problem. Moreover, it would be virtually impossible

[39] R. DeMillo, R. Kadel, and M. Marks, "What voters are asked to verify affects ballot verification: A quantitative analysis of voters' memories of their ballots" (2018). Available at https://ssrn.com/abstract=3292208.

[40] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman, "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" in *Proceedings of the 41st IEEE Symposium on Security and Privacy* (Jan. 2020), https://jhalderm.com/pub/papers/bmd-verifiability-sp20.pdf.

[41] Philip Kortum, Michael D. Byrne, and Julie Whitmore, "Voter Verification of BMD Ballots Is a Two-Part Question: Can They? Mostly, They Can. Do They? Mostly, They Don't" (Mar. 2020), https://arxiv.org/ftp/arxiv/papers/2003/2003.04997.pdf.

for officials to recognize the subtle signs of a BMD misprinting attack during a chaotic election in which there were widespread equipment malfunctions and other problems, as occurred in Georgia during the June 9, 2020 primary.[42]

45. Even if officials did suspect that the BMDs had been attacked, there would be no straightforward way to respond or recover. One possible response would be to delay certifying the election results and conduct a forensic analysis to understand why ballots were misprinted and how many BMDs and votes were affected. Such an analysis might take months and would not be guaranteed to uncover a sophisticated attack. Yet if an attack were confirmed, there is little chance that its effects could be undone. The only recourse might be to rerun the election, which could be statewide involving millions of voters across Georgia.

46. Election officials are unlikely to take disruptive actions, like a protracted and expensive forensic investigation, unless a large enough fraction of BMD voters report problems. Suppose officials would launch an investigation if more than 1% of BMD voters reported a problem. If outcome-changing fraud occurred in an election with a 1% margin of victory, voters would need to verify their ballots so

[42] Richard Fausset, Reid J. Epstein, and Rick Rojas, "'I Refuse Not to Be Heard': Georgia in Uproar Over Voting Meltdown," *The New York Times* (June 9, 2020), https://www.nytimes.com/2020/06/09/us/politics/atlanta-voting-georgia-primary.html.

carefully that they would report 67% of the modified BMD printouts. This is *ten times* greater than the rate of error reporting measured in my peer-reviewed research.

<u>Reserving BMDs for Voters Who Request Them Would Strengthen Security</u>

47. When BMDs are used by all in-person voters, as in Georgia, there is a high risk that attackers could manipulate enough BMD votes to change the outcome of a close election without detection. Georgia is an outlier in adopting BMDs for all voters. As of December 2019, only 403 counties in the United States planned to do so, and almost 40% of them were in Georgia.[43] In contrast, the majority of election jurisdictions across the U.S. (representing nearly two-thirds of registered voters) provide BMDs exclusively for voters who request them (e.g., those with certain disabilities),[44] which is much safer.

48. Georgia can greatly strengthen the security of future elections through a straightforward procedural change. Rather than directing all in-person voters to use BMDs, the State could have in-person voters mark paper ballots by hand and reserve BMDs for voters who request to use them. This approach would require no additional equipment and would result in no loss in accessibility. Hand-marked

[43] Decl. of Warren Stewart, Dckt. 681-2.

[44] Verified Voting, *The Verifier*, https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2020 (last visited Aug. 18, 2020).

paper ballots are already used in Georgia for absentee voting, and so they are prepared and printed for every ballot style in every election. The state's new Dominion scanners are already capable of counting hand-marked ballots. BMDs would continue to be available for voters who need them. Yet the risk that election outcomes could be hacked would be far less than under Georgia's planned system.

49. Securing against misprinting attacks is much easier if only a small fraction of voters uses BMDs (without barcodes) and the rest use hand-marked paper ballots. This is because an attacker would be forced to cheat on a much larger fraction of BMD ballots in order to achieve the same level of fraud. In Maryland, which uses hand-marked paper ballots but makes BMDs available to voters who request them, about 2% of voters use BMDs. If only 2% of voters used BMDs in the scenario above (¶ 46), 1% of BMD voters would report a problem even if voters noticed only 3.8% of errors. Empirical studies suggest that voters really do achieve this modest rate of verification accuracy, even though it is unlikely they can achieve the far greater accuracy required to detect fraud when all voters use BMDs.

50. Using BMDs for all voters has no practical security advantages compared to reserving BMDs for voters who request them. On the contrary, it makes BMDs a much more attractive target for attackers and leads to greatly increased risks

for all voters—including the disabled—that their right to vote will be subverted by an attack on the BMDs. And regardless, there is no need for barcodes at all.

Georgia's Audits Provide Insufficient Protection

51. Rigorous post-election audits are necessary in order to reliably prevent attacks that compromise election results by manipulating ballot scanners. A rigorous audit would also serve to correct errors caused by scanners misreading ballots, to the extent that these errors resulted in an incorrect election outcome. However, as I have explained, post-election audits are not sufficient to detect attacks against BMDs, since such attacks could change both the printed and electronic records of the votes.

52. For an audit to reliably detect outcome-changing attacks, several requirements must be met. Among them are: (i) the paper ballots being audited must correctly reflect voters' selections; (ii) the audit needs to be conducted manually, by having people inspect the ballots without reliance on potentially compromised electronic systems or records; (iii) the auditors need to inspect sufficiently many ballots to ensure that the probability that outcome-changing fraud could go undetected is low. In general, the closer the election result in a particular race, the more ballots need to be audited in order to confidently rule out fraud. Audits that constrain the probability that the reported outcome differs from the outcome that

would be obtained by a full manual recount to no more than a pre-defined level (the "risk limit") are called risk-limiting audits ("RLAs").[45]

53. I understand that Georgia statute requires a state-wide post-election audit to be conducted no later than the November 2020 election.[46] However, that audit is not required to be risk-limiting. If it is not, and there are close races in which an attacker changes the outcome by hacking the election equipment, there is a high probability that the audit will fail to uncover the attack.

54. A proposed rule change recently noticed by the State Elections Board would require all counties to participate in a risk-limiting audit, but only following November general elections in even-numbered years.[47] Other elections, including state-wide primaries and runoffs, are not included in the requirement. Moreover, under the proposed rule, the RLA would target only one contest, which would be selected by the Secretary of State. Adversaries could choose to attack any race in

[45] *See* Mark Lindeman and Philip B. Stark, "A Gentle Introduction to Risk-limiting Audits," in *IEEE Security and Privacy* (2012), https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

[46] *See* O.C.G.A. § 21-2-498(b).

[47] Georgia State Elections Board, "Notice of Intent to Post a Rule of the State Election Board, Title 183-1, *Rules of State Election Board*, Chapter 183-1-15, *Returns of Primaries and Elections* and Notice of Public Hearing" (Aug. 11, 2020), https://sos.ga.gov/admin/files/SEB%20Rule%20183-1-15-.02(2)%20and%20.04%20-%20To%20Post%20For%20Public%20Comment.pdf.

any election, and an attack would likely not be detected if it occurred in a contest that was not the target of the RLA or during an election for which no RLA was conducted. Even for the one contest every two years that would be audited, the proposed rule does not describe the auditing procedure in enough detail to evaluate its sufficiency. The specific process that election superintendents would follow to carry out the audit is yet to be defined.

55. No matter what auditing procedures Georgia applies, the state's widespread use of BMDs makes it possible for an attacker to undermine the integrity of the paper trail. Malware could cause the BMDs to print fraudulent selections, both in the barcode and the human-readable text. Such an attack would be impossible to detect by auditing the ballots, even with an RLA, because all records of the voter's intent would be wrong.

Hand-Marked Paper Ballots Are Much More Secure

56. Hand-marked paper ballots (HMPBs) are the most widely used voting technology in the United States. More than 65% of voters live in jurisdictions that use HMPBs as their primary in-person voting technology,[48] and all 50 states, including Georgia, use them for absentee voting. When used with modern precinct-

[48] Verified Voting, *The Verifier*.

count optical scanners and rigorous RLAs, HMPBs can provide much stronger security than BMD-printed ballots, especially those based on barcodes.

57. Virtually every class of attack that affects HMPBs also affects BMDs, but BMDs—especially those that use barcodes—additionally suffer from the serious possibility that malicious software will alter the voter's choices without detection. In contrast, HMPBs can be well secured using existing election technology and procedural controls.

58. It is true that voters using hand-marked paper ballots sometimes make errors. However, modern ballot scanners, such as Georgia's Dominion ICPs, can be programmed to detect the most common types of errors by voters, such as overvotes and undervotes. Where ballots are scanned in-precinct, and the scanners are programmed correctly, voters then have the opportunity to correct their ballots once the scanners report the errors. Scanners also sometimes misread voters' marks, but such errors—to the extent that they affected an election outcome—would be detected and corrected during risk-limiting audits, which are necessary in any event in order to safeguard against outcome-changing attacks.

Georgia Elections Continue to be Threatened by Sophisticated Adversaries

59. Georgia's election system continues to face a high risk of being targeted by sophisticated adversaries, including Russia and other hostile foreign

governments. These adversaries could attempt to hack the election system to achieve a variety of goals, including undermining the legitimacy of the democratic process and causing fraudulent election outcomes.

60. The Mueller Report recently outlined the scale and sophistication of Russia's efforts to interfere in the 2016 election, leaving no doubt that Russia and other adversaries will strike again.[49] The Special Counsel concluded principally that "[t]he Russian government interfered in the 2016 presidential election in sweeping and systematic fashion."[50] The report further explained that foreign actors "sought access to state and local computer networks by exploiting known software vulnerabilities on websites of state and local governmental entities."[51] The report also found that these foreign agents were successful in attacking at least one state and that their activities involved "more than two dozen states."[52] As noted prior to the Special Counsel's final report, Georgia was among the states that Russia targeted.[53]

[49] Special Counsel Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election (Volume I of II)*, United States Department of Justice (Mar. 2019), https://www.justice.gov/storage/report.pdf.
[50] *Id.* at 1.
[51] *Id.* at 50.
[52] *Id.*
[53] *See* Indictment ¶ 75, *United States v. Netyksho*, No. 1:18-cr-00215-ABJ, (D.D.C. July 13, 2018), ECF No. 1.

61. Russia has sophisticated cyber-offensive capabilities, and it has shown a willingness to use them to hack elections elsewhere even before 2016. For instance, according to published reports, during the 2014 presidential election in Ukraine, attackers linked to Russia sabotaged Ukraine's vote counting infrastructure, and Ukrainian officials succeeded only at the last minute in defusing vote-stealing malware that would have caused the wrong winner to be announced.[54]

62. Russia and other foreign governments continue to threaten Georgia's elections in 2020. As recently as this month, the U.S. Intelligence Community assessed that foreign threats to the 2020 election include "ongoing and potential activity" from Russia, China, and Iran, concluding that "[f]oreign efforts to influence or interfere with our elections are a direct threat to the fabric of our democracy."[55] These adversarial governments may "seek to compromise our election infrastructure

[54] Mark Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers," *The Christian Science Monitor* (June 17, 2014), https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

[55] Office of the Director of National Intelligence, "Statement by NCSC Director William Evanina: Election Threat Update for the American Public" (Aug. 7, 2020), https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

for a range of possible purposes, such as interfering with the voting process, stealing sensitive data, or calling into question the validity of the election results."[56]

63. Georgia's BMD-based election system does not achieve the level of security necessary to withstand an attack by these sophisticated adversaries. Despite the addition of a paper trail, it suffers from severe security risks much like those of the DRE-based election system it replaced. Like paperless DREs, Georgia's BMDs are vulnerable to attacks that have the potential to change all records of a vote.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 19th day of August, 2020 in Rushland, Pennsylvania.

J. ALEX HALDERMAN

[56] *Id.*